

## UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*

)

)

Case No. 24-823M(NJ)

information associated with certain Facebook and Instagram  
accounts that are stored at premises owned, maintained,  
controlled, or operated by Meta Platforms, Inc. ("Meta"), a  
company headquartered in Menlo Park, California.

)

**WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin  
*(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized):*

Please see Attachment B.

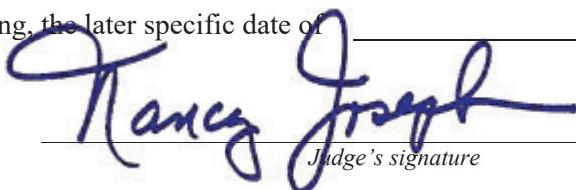
**YOU ARE COMMANDED** to execute this warrant on or before 3/28/2024*(not to exceed 14 days)* in the daytime 6:00 a.m. to 10:00 p.m.    xx at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph  
*(United States Magistrate Judge)*

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

for \_\_\_\_\_ days *(not to exceed 30)*     until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: 3/14/2024 @ 12:54 p.m.  
Judge's signatureCity and state: Milwaukee, WIHonorable Nancy Joseph, U.S. Magistrate Judge  
Printed name and title

**Return**

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

*Executing officer's signature*

\_\_\_\_\_  
*Printed name and title*

**ATTACHMENT A**  
**Property to Be Searched**

This warrant applies to information between September 1, 2023 and Present Date, associated with the following Facebook and/or Instagram Accounts:

- Target Facebook Account 1
  - Vanity Name: "Backed Up Rahriguez"
  - URL: <https://www.facebook.com/profile.php?id=100077294094771>
  - Facebook User ID: 100077294094771
- Target Instagram Account 1:
  - URL: [https://www.instagram.com/rahrieguez\\_backed\\_up/](https://www.instagram.com/rahrieguez_backed_up/)
  - Profile ID 64778292927,
- Target Instagram Account 2:
  - URL: <https://www.instagram.com/rahrahbackedup/>,
  - Profile ID 51699112134

that are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a social networking company headquartered in Menlo Park, California.

## **ATTACHMENT B**

### **Items to be Seized**

Information to be disclosed by Meta Platforms, Inc.

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Meta Platforms, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta Platforms, Inc. (“Meta”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in **Attachment A**:

- (a) All contact and personal identifying information, including the full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers for user Account Name with the Usernames and Account IDs listed in **Attachment A**.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook or Instagram activities from **September 1, 2023 to present**;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;

- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook/Instagram group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook/Instagram applications;
- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) All other records and contents of communications and messages made or received by the user from **September 1, 2023 thorugh present**, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
- (g) All "check ins" and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account's usage of the "Like" feature, including all Facebook/Instagram posts and all non-Facebook webpages and content that the user has "liked";
- (j) All information about the Facebook pages that the account is or was a "fan" of;
- (k) All past and present lists of friends created by the account;

- (l) All records of Facebook searches performed by the account from **September 1, 2023 through present**;
- (m) All information about the user's access and use of Facebook Marketplace;
- (n) The types of service used by the user;
- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook/Instagram posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) All records pertaining to communications between Facebook/Instagram and any person regarding the user or the user's Facebook/Instagram account, including contacts with support services and records of actions taken.
- (r) All content (whether created, uploaded, or shared by or with the Account), records, and other information relating to videos (including live videos and videos on IGTV), image stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from **September 1, 2023 to present**.
- (s) All content, records, and other information relating to communications sent from or received by the accounts in Attachment A including but not limited to:

- a. The content of all communications sent from or received by the Accounts listed in Attachment A, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available.
  - b. All records and other information about direct, group, and disappearing messages sent from or received by the Accounts listed in Attachment A including dates and times, methods, sources, and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot)
  - c. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants
  - d. All associated logs and metadata,
- (t) All content, records, and other information relating to all other interactions between the Accounts listed in Attachment A and other Instagram users from **September 1, 2023 through present** including but not limited to:
- a. Interactions by other Instagram users with the Accounts listed in Attachment A or its content, including posts, comments, like, tags, follows (including follows unfollows, approved and denied follow requests, and blocks and unblocks), shares invitations, and mentions
  - b. All users the Accounts listed in Attachment A has followed including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account

c. All contacts and related sync information

d. All associated logs and metadata

Meta is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18 U.S.C. § 2119 (carjacking) and Title 18 U.S.C. § 924(c)(use of a firearm during the commission of a violent crime), 18 U.S.C. § 922(g)(1) (unlawful possession of firearms and ammunition by a convicted felon) and 18 U.S.C. § 922(o) (unlawful transfer or possession of a machinegun) involving ROBERT H. HILL, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) The relevant offense conduct, any preparatory steps taken in furtherance of the scheme, communications between JOHN M. DAVIS, ROBERT H. HILL, ALVIN L. NICKSION and others related to the relevant offense conduct of illegal use and possession of firearms and carjacking;
- (b) Evidence indicating how and when the Facebook/Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook/Instagram account owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and
- (e) The identity of the person(s) who communicated with the user ID about matters relating to relevant offense conduct of the sale of firearms and sale and use of controlled substances, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**UNITED STATES DISTRICT COURT**  
for the  
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

Case No.24-823M(NJ)

information associated with certain Facebook and Instagram accounts  
that are stored at premises owned, maintained, controlled, or operated by  
Meta Platforms, Inc. ("Meta"), a company headquartered in Menlo Park,  
California.

**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2119	Carjacking
18 U.S.C. § 924(c)	Use of a Firearm during the Commission of a Violent Crime

The application is based on these facts:

Please see Affidavit.

Continued on the attached sheet.

Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

**FRANK RUTTER** Digitally signed by FRANK RUTTER  
Date: 2024.03.13 10:55:14 -05'00'

*Applicant's signature*

**Frank Rutter, Special Agent - ATF**

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone \_\_\_\_\_ (*specify reliable electronic means*).

Date: 3/14/2024 @ 12:55 p.m.

City and state: Milwaukee, WI

*Nancy Joseph*  
Judge's signature

**Honorable Nancy Joseph, U.S. Magistrate Judge**

*Printed name and title*

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION FOR SEARCH WARRANTS**

I, Frank Rutter, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain Facebook and Instagram accounts that are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), a company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

2. I am employed with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been since 2015. As an ATF Agent, I have participated in the investigation of firearms and narcotics-related offenses, resulting in the prosecution and conviction of numerous individuals and the seizure of illegal drugs, and weapons. As a firearms investigator, I have interviewed many individuals involved in firearm and drug trafficking and have obtained information from them regarding acquisition, sale, importation, manufacture, and distribution of firearms and controlled substances. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology utilized by the traffickers and abusers of controlled substances.

3. I have completed approximately 26 weeks of training at the Federal Law

Enforcement Training Center in Glynco, Georgia, as well as the ATF National Academy. That training included various legal courses related to constitutional law as well as search and seizure authority. Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as interviewing, surveillance, and evidence collection.

4. Based on my training, experience and participation in drug trafficking and firearms trafficking investigations, I know and have observed the following:

5. I have relied on informants to investigate firearms trafficking and drug trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have learned about the manner in which individuals and organizations finance, purchase, transport, and distribute firearms and narcotics both within and outside of Wisconsin. I have utilized informants to conduct “controlled purchases” of firearms and controlled substances from individuals, as opposed to licensed gun dealers. I have also conducted surveillance of individuals engaged in firearms and drug trafficking and participated in the execution of numerous search warrants resulting in the seizure of drugs, firearms, ammunition, and magazines.

6. During the course of my career, I have conducted criminal investigations involving the use of social media. Additionally, I have received training and instruction regarding the use of social media sites by criminal elements. I have conducted previous criminal investigations in which internet research that I conducted yielded the use of social media by suspects. Specifically, I know from my training and experience that alleged suspects of criminal activity, who have accounts on social media websites, will often communicate their criminal intentions or past activity via “instant message” or “in-box message” on a given social media website. The “instant message” / “in-box message” is a private communication from one user to another. Furthermore, I know

through experience that many social media users often use social media websites as their primary means to communicate with others. Additionally, I know from training and experience that suspects who use social media websites sometimes post photographs of themselves possessing incriminating items, such as narcotics, unexplained large amounts of cash, and firearms. Also, suspects in criminal investigations have been known to post statements and/or lyrics on social websites referencing their own criminal activity

7. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

8. There is probable cause to believe that evidence of violations of the following laws of the United States, including the things described in Attachment B, will be found in the property listed in Attachments A, respectively: Title 18 U.S.C. § 2119 (carjacking) and Title 18 U.S.C. § 924(c)(use of a firearm during the commission of a violent crime), 18 U.S.C. § 922(g)(1) (unlawful possession of firearms and ammunition by a convicted felon) and 18 U.S.C. § 922(o) (unlawful transfer or possession of a machinegun)

### **PROBABLE CAUSE**

#### **October 26, 2023 Carjacking (Location 1 and 2)**

9. On October 26, 2023, the Milwaukee Police Department (MPD) responded to an armed carjacking which occurred at 3915 S. Logan Avenue, Milwaukee, Wisconsin (Location 1). When officers arrived the spoke to the victim, identified as B.F. (DOB XX/XX/1989) who stated he was seated in the driver's seat of his vehicle, a gray 2018 Volkswagen Passat sedan (bearing

Wisconsin license plate ARV1960), using an iPad for work purposes. B.F. stated at approximately 5:20 pm (CST) he observed an unknown black male (suspect 1) walk up to his front driver's door, open the closed door, and order him out of the vehicle. B.F. stated suspect 1 pointed, what B.F. believed to be, a black semi-automatic with a light-colored grip, at his head. B.F. stated he complied and exited the vehicle. B.F. stated after he got out of the vehicle, suspect 1 grabbed him and pulled him to the middle of S. Logan Avenue and asked B.F. what other property he possessed. B.F. stated he told suspect 1 he had a wallet and suspect 1 took the wallet from him. B.F. stated suspect 1 then got into the driver seat of the aforementioned Volkswagen sedan, and another black male (suspect 2), got into the front passenger seat. B.F. stated the suspects then drove away west bound in the alley from S. Logan Avenue.

10. B.F. described suspect 1 as a black male, late teens to early 20's, approximately 5'10", skinny build, wearing a charcoal gray hooded sweatshirt with the hood up, and blue jeans with different shades. B.F. stated the sweatshirt had a large lighter colored emblem on the chest.

11. B.F. described suspect 2 as a black male, unknown age, approximately 5'04" to 5'07", skinny build, wearing a dark gray hooded sweatshirt with the hood up.

12. MPD detectives later spoke to witness J. N. who stated she observed two black males, wearing hooded sweatshirts enter a gray vehicle and drive away. Detectives located and viewed ring doorbell footage which corroborated the victim's statement of events. Detectives describe suspect 1 as black male, approximately 5'10", skinny build, wearing a dark colored hooded sweatshirt with a large white or light-colored chest emblem on it, possibly blue jeans, and dark shoes. Suspect 2 was observed to be a black male, approximately 5'05", skinny build, wearing a light gray hooded sweatshirt with the hood up, dark pants, and white or light-colored shoes.

13. A short time later, MPD responded and talked to a witness, N.S. N.S. stated at approximately 05:30 pm, they were jogging westbound on E. Howard Avenue past S. Pine Avenue, when he located an Apple iPhone in the middle of the sidewalk on the north end of E. Howard Ave. just west of S. Pine Avenue (Location 2). N.S. stated he called the number displayed on the phones lock screen and it resulted in MPD being dispatched to his location. The phone was determined by MPD to be B.F.'s phone, which was inside his vehicle during the carjacking, and was subsequently returned to B.F.

#### **Auto Zone Purchase (Location 3)**

14. While conducting their investigation into the October 26, 2023 carjacking of the aforementioned Volkswagen Passat sedan, Detectives determined the vehicle was spotted at an Auto Zone, located at 208 E. Capitol Drive, Milwaukee, Wisconsin (Location 3), on October 27, 2023 at 12:38 pm (CST). Video footage collected from the business depicts the aforementioned Volkswagen Passat sedan arrive and park in the parking lot of the business. MPD Detective Michael Martin observed the front passenger exit the vehicle. Det. Martin recognized this individual to be Suspect 1 from the carjacking on October 26, 2023. The surveillance footage further depicted Suspect 1 enter the store and purchase a roll of window tint, which the suspect pays for by utilizing his phones tap-to-pay feature, at the register. Suspect 1 then exits the store, gets back into the front passenger seat of the Passat, and the vehicle drives away.

15. Det. Martin further described Suspect 1, from the surveillance video, as a black male, approximately 20 years old, 5'10" to 6'00", skinny build, dark complexion, wearing a black "pooh sheisty" pull over head mask, a black hooded sweatshirt with a cartoon "Popeye the Sailor Man" emblem on it, black jogging pants with a vertical gray stripe on the side, and a possible

Milwaukee Bucks deer head logo on the stripe, electric blue underwear, black shoes and white socks.

**October 27, 2023 Fleeing/Eluding MPD (Location 4 and 5)**

16. On October 27, 2023, at approximately 5:53 pm (CST), MPD observed a vehicle matching the description of the aforementioned Volkswagen Passat, which officers knew to be stolen, driving southbound on N. 51<sup>st</sup> Street from W. Capitol Avenue (Location 4). MPD Officers initiated a traffic stop, in their fully marked MPD squad, and the vehicle failed to stop and fled from officers at a high rate of speed. MPD maintained visual contact of the vehicle until the pursuit ended in the area of 2301 N. 18<sup>th</sup> Street (Location 5), when the vehicle stopped, and four occupants fled on foot. MPD gave chase and arrested two of the four occupants the vehicle. The occupants were further described as:

- Driver of the vehicle, arrested and identified as John M. DAVIS (B/M, XX/1997), wearing a dark colored hooded sweatshirt with a “Glock” firearms brand graphic and white writing with the text “No Gun, No Fun” on the back of the sweatshirt.
- Rear driver side passenger, arrested and identified as Willie E. ADAMS (B/M, DOB 12/02/1997)
- Front passenger, black male, wearing a black hooded sweatshirt, red track pants with white stripes
- Rear passenger side passenger, black male, wearing a black hooded sweatshirt, black pants and blue underwear

**Timing Advanced Area Searches and Tower Dumps**

21. On November 06, 2023, the Honorable William Duffin, U.S. Magistrate Judge in the Eastern District of Wisconsin signed a search warrant and court order which authorized Timing Advance Area Searches and tower dumps in relation to the offenses listed above. These warrants returned thousands of lines of cellular data and information which was then analyzed to initially identify only those identifiers whose records were consistent with the facts of the investigation, including being in the geographic area of more than one location. As a summary the following locations were queried:

- Location 1 – 3915 S. Logan Ave, Milwaukee, Wisconsin on October 26, 2023
- Location 2 – Intersection of E. Howard Avenue and S. Pine Avenue, Milwaukee, Wisconsin on October 26, 2023
- Location 3 – 208 E. Capital Drive, Milwaukee, Wisconsin on October 27, 2023
- Location 4 – Intersection of N. 51st Blvd. and W. Capitol Drive, Milwaukee, Wisconsin on October 27, 2023
- Location 5 – 2301 N. 18th Street, Milwaukee, Wisconsin on October 27, 2023

#### **Analysis of Timing Advanced Area Searches and Tower Dumps**

22. The information was analyzed by the Federal Bureau of Investigation (FBI) Cellular Analysis Team who provided the information to the affiant and summarized the info below as to the identification of **(414) 435-6392 (Suspect Device 1)**, **(414) 416-3779 (Suspect Device 2)**, and **(414) 539-8890 (Suspect Device 3)**.

23. The initial review provided to the affiant for the US Cellular and AT&T returns provided an initial list of approximately **twenty (20) phone numbers** which hit at least two (2) of the five (5) locations which would include records around the carjacking locations (Location 1 and

2) **and** any of the other locations which include the Auto Zone (Location 3) and Fleeing/Eluding (Location 4 and 5). This initial analysis was done due to the largest distance being between the carjacking locations and other points. Your affiant notes that the 20 phone numbers were provided to him out of thousands of other identifiers and included **Suspect Device 2** and **(414) 539-8890 Suspect Device 3**. Furthermore, **Suspect Device 3** was noted to have had records at three (3) locations.

24. After reviewing the initial information from AT&T and US Cellular your affiant received the results from T-Mobile which were then analyzed and revealed that a unique **International Mobile Subscriber Identity (IMSI) 310260685268367** had records within all five (5) search locations. Additionally, the tower dump records were reviewed for that IMSI which showed the associated phone number for that IMSI as **(414) 435-6392 (Suspect Device 1)**.

25. Your affiant notes that the Timing Advance area searches provide more detailed location information for the cellular devices, but communications such as voice and text are contained within the tower dump records. The tower dump records were reviewed, and it was identified that **Suspect Device 1** and **Suspect Device 2**, both had phone contact with the phone number **(414) 539-8890 (Suspect Device 3)**. Additionally, **Suspect Device 3** was identified as having records at three (3) locations and within the initial 20 phone numbers provided to your affiant.

26. In summary, the Suspect Devices have records in the below locations and communication with each other as noted below. Your affiant further notes that for the purpose of the analysis the two locations for the carjacking (Location 1 and Location 2) are extremely close in proximity and are summarized as a single location/event below.

- a. **Suspect Device 1:** Records within all five (5) search areas (4 main locations) and communication with (414) 539-8890 (Suspect Device 3)
- b. **Suspect Device 2:** Records within two (2) main locations – Carjacking and AutoZone and communication with (414) 539-8890 (Suspect Device 3)
- c. **Suspect Device 3:** Records within three (3) main locations – Carjacking and two (2) Fleeing/eluding and communication with (414) 435-6392 (Suspect Device 1) and (414) 416-3779 (Suspect Device 2)

27. Based on the multiple locations for all the Suspect Devices, including all Suspect Devices having records in the geographic area of the carjacking, in addition to the Suspect Devices being in contact with another as noted above, there is probable cause to believe that the users of the Suspect Devices are involved in the violations being investigated and that obtaining both historical and prospective location information will provide evidence of the violations including but not limited to the identities of the subjects, and the locations where they live and the physical cellular device both which can contain additional evidence related to the investigation.

**John M. DAVIS as the user of (414) 435-6392 (Suspect Device 1)**

28. Following the arrest of John M. DAVIS on October 27, 2023, MPD Detectives conducted a mirandized interview with DAVIS. DAVIS stated there were four occupants inside the aforementioned Volkswagen sedan during the pursuit, and he admitted to being the driver. DAVIS stated he did not know the car was stolen and was fleeing because he did not have a valid driver's license. Davis stated the car belonged to the neighbor of his girlfriend, whom DAVIS knew only as "K". DAVIS described "K" as a black male, and DAVIS stated "K" was in the front passenger seat of the vehicle at the time of the pursuit. DAVIS stated he had two phones that belonged to him in his possession during the pursuit. DAVIS stated he had an Apple iPhone 11

with no case, with the phone number of "(414) 425-6392". It should be noted, **Suspect Device 1** has the phone number **(414) 435-6392**, leading your affiant to conclude DAVIS changed one digit in an attempt to conceal the true number from MPD.

29. Your affiant queried recorded jail calls placed from the Milwaukee County Jail to **Suspect Device 1** and determined inmate John DAVIS placed one call to **Suspect Device 1** on October 31, 2023, and one call on November 1, 2023. Your affiant also learned John DAVIS placed 44 calls to **Suspect Device 2**, while in custody, between October 29, 2023, and December 19, 2023, and 53 calls to **Suspect Device 3**, while in custody, between November 01, 2023, and December 19, 2023.

30. On October 29, 2023, DAVIS placed a recorded phone call to an unknown male using **(414) 416-3779 (Suspect Device 2)**. During the phone conversation, DAVIS directs the unknown male to hold onto the phone for him while he is in custody, and the unknown male agrees. During this call, DAVIS self-identified himself. In numerous other jail calls placed to **(414) 416-3779 (Suspect Device 2)** between October 29, 2023 and November 12, 2023, DAVIS directs this same unknown male to go into DAVIS' phone and provide him with various phone numbers, which the unknown male does.

**Alvin L. NICKSION as the user of (414) 416-3779 (Suspect Device 2)**

31. On December 04, 2023, your affiant queried the telephone number **(414) 416-3779 (Suspect Device 2)** through North Central High Intensity Drug Trafficking Area (HIDTA), a state and federal law enforcement taskforce. Your affiant was notified by North Central HIDTA, that this number was identified in HIDTA reports and HIDTA case management software as active number pertaining to an ongoing Milwaukee Police Department narcotics investigation. Your

affiant spoke to MPD Det. John Schott, who stated the MPD had determined that the current user of **Suspect Device 2** is identified as Alvin NICKSION (b/m, DOB XX/XX/1991).

- a. A search of NICKSION's criminal history revealed he has previous felony convictions in the state of Wisconsin for Burglary Any Building or Dwelling, and Retail Theft.
- b. A search of Wisconsin DMV records list NICKSION's residence as 1128 W. Keefe Avenue, Milwaukee, Wisconsin (**PREMISES 1**), which is in the Eastern District of Wisconsin.
- c. A search of common law enforcement databases also listed NICKSION as residing at 1128 W. Keefe Avenue, Milwaukee, Wisconsin (**PREMISES 1**) from June of 2012 to present.
- d. Analysis of historical location data collected for **Suspect Device 2** revealed the phone was pinging on a cellular tower that covered 1128 W. Keefe Avenue, Milwaukee, Wisconsin (**PREMISES 1**) during the overnight hours every night from January 15, 2024, to January 21, 2024, as well as the overnight hours of January 23, 2024. The historical records which were analyzed did not include data past January 23, 2024.
- e. On January 25, 2024, ATF personnel conducted a trash pull at 1128 W. Keefe Avenue, Milwaukee, Wisconsin (**PREMISES 1**), but no mail was recovered.

#### **Recovery of Cellular Phones**

32. On December 08, 2023, personnel from HIDTA and Milwaukee Metropolitan Drug Enforcement Group (MMDEG) executed a state search warrant at 2200 N. 31st Street, unit 117.

Alvin NICKSION was present at this location during the warrant execution, and during search, investigators located three (3) cellular phones, one (1) round of .40 caliber ammunition, a pistol brace, two (2) pill bottles containing suboxone strips, and a multi-colored zip lock style dispensary bag that contained 2.79 grams of green leafy substance which was consistent in appearance with marijuana. The cellular phones were located in a bedroom which contained NICKSION's clothing and other personal effects.

33. Investigators subsequently obtained a state search warrant on January 10, 2024 for two (2) of the cellular phones recovered in the aforementioned warrant. Det. Schott later provided details to SA Rutter that TARGET CELL PHONE 2, was found to have the phone number (414) 435-6392 (Suspect Device 1) and was registered to Apple ID: johndavism97@gmailcom. Your affiant is aware DAVIS directed NICKSION to hold onto his phone, which is Suspect Device 1, while DAVIS was in custody. The two cellular devices are more particularly described as:

- a. Blue Apple iPhone (unknown model, unknown serial number, contained on Milwaukee Police Department Inventory No. 24000904, Item 1, **TARGET CELL PHONE 1**)
- b. Black Apple iPhone with "Backwoods" branded case (model unknown, serial no. unknown, contained on Milwaukee Police Department Inventory no . 24000904 item 2, **TARGET CELL PHONE 2**)

34. On January 08, 2024, the Honorable William Duffin, U.S. Magistrate Judge in the Eastern District of Wisconsin signed a search warrant which allowed for the real-time collection of location data for **(414) 416-3779 (Suspect Device 2)**. The warrant also provided for the

collection of historical location data for **Suspect Device 2**. The warrant is set to expire on February 7, 2024.

35. On January 19, 2023, location data for **Suspect Device 2** indicated the device was pinging on a cellular tower which covered 1128 W. Keefe Avenue (**PREMISES 1**). ATF personnel responded and conducted surveillance in the area of 1128 W. Keefe Avenue (**PREMISES 1**). Between approximately 08:40 AM and 09:15 AM CST, your affiant observed a black male, wearing a black winter jacket and pants, and a black hat shoveling snow outside 1128 W. Keefe Avenue (**PREMISES 1**). The unknown male had the same build (i.e. height, weight, hair color, skin tone) as NICKSION. During this time, ATF SA Jody Keeku observed the male enter and exit both the front and side door to the residence freely without keys on numerous occasions.

**Robert H. HILL as the user of (414) 539-8890 (Suspect Device 3)**

36. On January 08, 2024, the Honorable William Duffin, U.S. Magistrate Judge in the Eastern District of Wisconsin signed a search warrant which allowed for the real-time collection of location data for **(414) 539-8890 (Suspect Device 3)**. The warrant also provided for the collection of historical location data for **Suspect Device 3**. The warrant is set to expire on February 7, 2024.

37. On January 18, 2024, MPD Ofc. Chris Randazzo listened to a Milwaukee County Jail call placed on January 07, 2024 by an inmate of the Milwaukee County Jail to an unknown male utilizing the number **(414) 539-8890 (Suspect Device 3)**. During the call, the possessor of **Suspect Device 3** stated they currently had a court hearing scheduled for sentencing on February 22, 2024. Ofc. Randazzo then queried open court cases for sentencing which were scheduled for

that date and learned Robert H. HILL (b/m, DOB XX/XX/1996), had a sentencing scheduled for that date. Ofc. Randazzo recognized HILL from prior law enforcement contacts he had with HILL, and Ofc. Randazzo knew HILL resided in the area of 38<sup>th</sup> and W. Galena Street in Milwaukee, Wisconsin. Ofc. Randazzo was also aware that historical location data collected for **Suspect Device 3** was regularly pinging on a cellular tower which covered the area of 38<sup>th</sup> and W. Galena Street, during overnight hours, throughout the warranted collection period, which lead him to believe the possessor of the device lived in that area. Ofc. Randazzo also knows that MPD has HILL as a documented associate of John DAVIS.

- a. A query for utilities with We Energies revealed, HILL was the account holder for 3809 W. Galena Street, Milwaukee, Wisconsin (**PREMISES 2**), which is in the Eastern District of Wisconsin.
- b. A search of HILL's criminal history revealed prior state of Wisconsin felony convictions for Armed Robbery and Prohibited Possession of a Firearm.

38. On January 19, 2024, ATF personnel conducted surveillance in the area of 3809 W. Galena Street, Milwaukee, WI (**PREMISES 2**). All personnel reviewed photographs of HILL prior to surveillance. At approximately 08:59 AM (CST), ATF SA Ricky Hankins observed HILL, exit 3809 W. Galena Street and walk to ABC Liquor, located at 1606, N. 35<sup>th</sup> Street, Milwaukee, WI. HILL was wearing a black mask over his mouth, a black puffy coat, and dark colored sweatpants. SA Hankins photographed HILL and your affiant later positively identified the male as HILL as well.

39. At 09:03 AM (CST), location data for **Suspect Device 3**, indicated the device was no longer at the residence and had moved a short distance in a manner consistent with a subject walking.

40. At approximately 09:09 AM (CST), ATF SA Paul Kozelek observed HILL exit the store and walk directly back to 3809 W. Galena Street (**PREMISIS 2**). SA Hankins then observed HILL enter the residence through the unlocked door marked “3809.”

41. At 09:19 AM (CST), location data for **Suspect Device 3**, indicated the device was once again pinging at the residence, just as it had been prior to HILL’s trip to ABC Liquors. This leads your affiant to conclude HILL was in possession of the device belonging to cellular phone number **Suspect Device 3**.

42. Analysis of historical location data collected for **Suspect Device 3** revealed the phone was pinging on a cellular tower that covered 3809 W. Galena Street (**PREMISIS 2**) during the overnight hours on nightly basis, between January 20, 2024 through January 25, 2024.

43. On January 30, 2024, Affiant conducted further surveillance on the premises at 3809 West Galena Street (**PREMISES 2**) and observed that the garage is affixed with the numbers “3809,” which correspond with the lower unit. The numbers corresponding with the upper unit were not visible on the garage.

44. On January 30, 2024, the Honorable William Duffin, U.S. Magistrate Judge in the Eastern District of Wisconsin signed a search warrant permitting the search and seizure of evidence from PREMISES 1, PREMISES 2 and the persons of Alvin NICKSION and Robert HILL.

45. On February 1, 2024 those search warrants were executed. Recovered from the search warrant scenes included, but was not limited to, numerous cellular devices, firearms, and

ammunition. One firearm in particular can be described as a tan over black Glock pistol bearing serial number BSCA405 which was recovered from Alvin NICKSION.

46. Alvin NICKSION was arrested by the Milwaukee Police Department during the search for being a felon in possession of a firearm which had been located between the driver's seat and center console of the vehicle NICKSION attempted to utilize to flee from law enforcement during the search warrant execution. During a subsequent mirandized interview with NICKSION, he stated he had no knowledge of the firearm and denied it belonged to him. NICKSION consented to providing a DNA sample to corroborate his statements.

47. Robert HILL was not arrested and declined to be interviewed by agents.

48. On March 4, 2024, SA Rutter located publicly visible Facebook account bearing vanity name "Backed Up Rahriguez" with Facebook User ID: 100077294094771 (**TARGET FACEBOOK ACCOUNT 1**). SA Rutter compared photographs from the aforementioned Facebook page with a Milwaukee Police Department (MPD) booking photograph for Robert HILL and found the images to be consistent and representative of the same individual. Also observed were numerous posts advising the birthday of the account user was the same date (no year specified) as HILL.

49. A review of publicly visible photographs revealed several images showing HILL wearing a black hooded sweatshirt depicting "Popeye the Sailor" on the front. One of the images

showed HILL wearing a black ski mask in addition to the hooded sweatshirt. These images were dated March 16, 2022. Below are screenshots from HILL's Facebook account.



50. Your affiant is aware one of the suspects in the armed robbery carjacking that occurred on October 26, 2023 was wearing a black ski-mask and a black hooded sweatshirt with a "Popeye the Sailor" logo on it. Below is screenshot from Autozone's DVR depicting one of the carjacking suspects on October 27, 2023.



51. HILL's profile picture depicted him alongside John DAVIS. HILL could be seen possessing what appeared to be a Glock pistol with a machinegun conversion device (MCD), commonly referred to as a "switch," affixed to the rear of the pistol slide. The image was posted on November 20, 2023.



52. The color of the pistol being tan over black is consistent with the Glock pistol recovered from Alvin L. NICKSION (B/M, 12/14/1991) during a federal search warrant on February 1, 2024.

53. On March 6, 2024, SA Rutter reviewed data forensically extracted from a cellular device that was seized pursuant to a Wisconsin state search warrant on December 12, 2023 from Alvin NICKSION. On February 21, 2024, The Honorable Stephen Dries, U.S. Magistrate Judge in the Eastern District of Wisconsin signed a federal search warrant permitting investigators to review the data obtained through the aforementioned Wisconsin state search warrant. Discovered during review of the electronic contents was the aforementioned photograph from HILL's Facebook page (**TARGET FACEBOOK ACCOUNT 1**) depicting HILL, DAVIS and the suspected Glock pistol with a MCD. The metadata for that photograph revealed it was taken in the rear of 1128 W. Keefe Avenue in Milwaukee, Wisconsin (PREMISES 1) on October 7, 2023. The image was taken with an iPhone 14 that was registered with Apple ID account:

[shawnlowend@icloud.com](mailto:shawnlowend@icloud.com). Your affiant is aware NICKSION stated he regularly used the nickname “shawn” during a mirandized interview with MPD and ATF on February 2, 2024.

54. Also discovered within the contents of the electronic device was a close-up image of what appeared to be the same Glock pistol with the MCD attached. The metadata for the image revealed it to have been taken in Milwaukee, Wisconsin on October 4, 2023. The image was of sufficient quality to read the serial number as BSCA405. Your affiant is aware this firearm was recovered from Alvin NICKSION on February 1, 2024 during a federal search warrant (See Paragraphs 44-46). It should be noted the firearm was not recovered with the MCD.

55. Robert HILL is a previously convicted felon based on felony convictions in the state of Wisconsin based on Milwaukee County cases 2013CF001467 and 2016CF001977 for Armed Robbery and Felon in Possession of a Firearm, respectively. As a result of these convictions he is federally prohibited from possessing any firearms or ammunition.

56. Also observed on the aforementioned Facebook was reference to HILL’s Instagram account. SA Rutter located two Instagram accounts for HILL bearing usernames “rahrieguez\_backed\_up” (User ID 64778292927) and “rahrahbackedup” (User ID: 51699112134). Both of these Instagram accounts displayed the same profile image as HILL’s Facebook account depicting him possessing what appeared to be a Glock pistol with a machinegun conversion device (MCD), commonly referred to as a “switch,” affixed to the rear of the pistol slide.

57. Your affiant knows from training and experience that it is common for those engaged in illegal firearm possession to utilize social media to display their firearms as well as enhance their social stature within their peer group.

#### **TECHNICAL INFORMATION**

58. Based on my training and experience, I am aware that individuals involved in criminal activity, including violent offenses with firearms, have also used websites and third-party applications, such as Facebook and Instagram, to communicate regarding their illegal activity and flaunt illegal firearms.

59. Meta Platforms, Inc. owns and operates the free-access social networking websites called Facebook and Instagram that can be accessed at <http://www.facebook.com> and <http://www.Instagram.com> respectively. Facebook/Instagram allow its users to establish accounts with Facebook/Instagram, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook/Instagram users, and sometimes with the general public.

60. Facebook/Instagram asks users to provide basic contact and personal identifying information to Facebook/Instagram, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook/Instagram passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook/Instagram also assigns a user identification number to each account.

61. Facebook/Instagram also collects and retains information about how each user accesses and uses Facebook/Instagram. This includes information about the IP addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

62. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same

usernames at the same time. Instagram users can create multiple accounts and, if “added” to the primary account, can switch between the associated accounts on a device without having to repeatedly log in and log out.

63. Instagram users can also connect their Instagram and Facebook accounts to use certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Facebook maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Facebook and third-party websites and mobile apps.

64. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

65. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other

users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

66. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

67. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

68. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

69. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

70. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

71. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

72. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

73. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

74. Instagram users have several ways to search for friends and associates to follow on Instagram, such as by allowing Facebook to access the contact list on their devices to identify which contacts are Instagram users. Facebook retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Facebook to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates

75. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on the privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("bio"), and a website address.

76. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or store on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of others ("tag"), or add a location. These appear as posts on the user's profile. Users can remove

posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Facebook servers.

77. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are “tagged” in a post by its creator or mentioned in a comment (user can “mention” others by adding their username to a comment followed by “@”). An Instagram post created by one user may appear on the profile or feeds of other users depending on several factors including privacy settings and which users were tagged or mentioned.

78. An Instagram “story” is like a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator’s “Story Archive” and remain on Facebook servers unless manually deleted. The usernames of those who viewed a story are visible to the story’s creator until 48 hours after the story was posted.

79. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram’s long-form video app.

80. Instagram’s direct messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with “disappearing” photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can’t view their disappearing messages after they are sent but do have access to each message status,

which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

81. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform, Facebook, and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

82. Instagram has a search function which allows users to search for accounts by username, user activity by location and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be “followed” to generate related updates from Instagram. Facebook retains records of a user’s search history and followed hashtags.

83. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

84. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

85. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile,

that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

86. Facebook collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Facebook to personalize and target advertisements.

87. Social networking providers like Meta Platforms, Inc. typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook or Instagram users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta Platforms, Inc. typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

88. As explained herein, information stored in connection with a Facebook or Instagram account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook or Instagram user's IP log, stored electronic communications, and other data retained by Meta Platforms, Inc., can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private

messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook or Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses; investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Lastly, Facebook or Instagram account activity may provide relevant insight into the Facebook/ Instagram account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook/ Instagram account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

89. Therefore, the computers of Meta Platforms, Inc. are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook/Instagram, such as account access information, transaction information, and other account information.

## **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

90. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## **CONCLUSION**

91. Based on the foregoing, I request that the Court issue the proposed search warrant.

92. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta Platforms, Inc. Because the warrant will be served on Meta Platforms, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

93. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

94. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant

**ATTACHMENT A**  
**Property to Be Searched**

This warrant applies to information between September 1, 2023 and Present Date, associated with the following Facebook and/or Instagram Accounts:

- Target Facebook Account 1
  - Vanity Name: "Backed Up Rahriguez"
  - URL: <https://www.facebook.com/profile.php?id=100077294094771>
  - Facebook User ID: 100077294094771
- Target Instagram Account 1:
  - URL: [https://www.instagram.com/rahrieguez\\_backed\\_up/](https://www.instagram.com/rahrieguez_backed_up/)
  - Profile ID 64778292927,
- Target Instagram Account 2:
  - URL: <https://www.instagram.com/rahrahbackedup/>,
  - Profile ID 51699112134

that are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a social networking company headquartered in Menlo Park, California.

## **ATTACHMENT B**

### **Items to be Seized**

Information to be disclosed by Meta Platforms, Inc.

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Meta Platforms, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta Platforms, Inc. (“Meta”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in **Attachment A**:

- (a) All contact and personal identifying information, including the full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers for user Account Name with the Usernames and Account IDs listed in **Attachment A**.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook or Instagram activities from **September 1, 2023 to present**;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;

- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook/Instagram group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook/Instagram applications;
- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) All other records and contents of communications and messages made or received by the user from **September 1, 2023 thorough present**, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
- (g) All "check ins" and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account's usage of the "Like" feature, including all Facebook/Instagram posts and all non-Facebook webpages and content that the user has "liked";
- (j) All information about the Facebook pages that the account is or was a "fan" of;
- (k) All past and present lists of friends created by the account;

- (l) All records of Facebook searches performed by the account from **September 1, 2023 through present**;
- (m) All information about the user's access and use of Facebook Marketplace;
- (n) The types of service used by the user;
- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook/Instagram posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) All records pertaining to communications between Facebook/Instagram and any person regarding the user or the user's Facebook/Instagram account, including contacts with support services and records of actions taken.
- (r) All content (whether created, uploaded, or shared by or with the Account), records, and other information relating to videos (including live videos and videos on IGTV), image stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from **September 1, 2023 to present**.
- (s) All content, records, and other information relating to communications sent from or received by the accounts in Attachment A including but not limited to:

- a. The content of all communications sent from or received by the Accounts listed in Attachment A, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available.
  - b. All records and other information about direct, group, and disappearing messages sent from or received by the Accounts listed in Attachment A including dates and times, methods, sources, and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot)
  - c. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants
  - d. All associated logs and metadata,
- (t) All content, records, and other information relating to all other interactions between the Accounts listed in Attachment A and other Instagram users from **September 1, 2023 through present** including but not limited to:
- a. Interactions by other Instagram users with the Accounts listed in Attachment A or its content, including posts, comments, like, tags, follows (including follows unfollows, approved and denied follow requests, and blocks and unblocks), shares invitations, and mentions
  - b. All users the Accounts listed in Attachment A has followed including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account

c. All contacts and related sync information

d. All associated logs and metadata

Meta is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18 U.S.C. § 2119 (carjacking) and Title 18 U.S.C. § 924(c)(use of a firearm during the commission of a violent crime), 18 U.S.C. § 922(g)(1) (unlawful possession of firearms and ammunition by a convicted felon) and 18 U.S.C. § 922(o) (unlawful transfer or possession of a machinegun) involving ROBERT H. HILL, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) The relevant offense conduct, any preparatory steps taken in furtherance of the scheme, communications between JOHN M. DAVIS, ROBERT H. HILL, ALVIN L. NICKSION and others related to the relevant offense conduct of illegal use and possession of firearms and carjacking;
- (b) Evidence indicating how and when the Facebook/Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook/Instagram account owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and
- (e) The identity of the person(s) who communicated with the user ID about matters relating to relevant offense conduct of the sale of firearms and sale and use of controlled substances, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.